IN THE UNITED STATED DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

ZOHO CORPORATION,	§	
	§	
Plaintiff,	§	
	§	
v.	§	Case No. 1:22-cv-0037
	§	
LIBERTY PEAK VENTURES, LLC,	§	JURY DEMANDED
	§	
Defendant.	§	

LIBERTY PEAK VENTURES, LLC,	§	
	§	
Counterclaimant,	§	
	§	
v.	§	
	§	
ZOHO CORPORATION,	§	
	§	
Counter-Defendant	§	
	§	
and	§	
	§	
ZOHO CORPORATION PVT. LTD	§	
	§	
Third-Party Defendant.	§	
	§	
.	§	

LIBERTY PEAK VENTURES, LLC'S
COUNTERCLAIM AND THIRD-PARTY COMPLAINT

This is a Counterclaim and Third-Party Complaint for patent infringement arising under the patent laws of the United States of America, 35 U.S.C. § 1 et seq. in which Counterclaimant and Third-Party Plaintiff Liberty Peak Ventures, LLC ("LPV" or "Counterclaimant"), by and

through the undersigned counsel, hereby make the following allegations of patent infringement relating to U.S. Patent Nos. 9,373,122 (the "'122 Patent"), 10,074,088 (the "'088 Patent"), and 10,956,901 (the "'901 Patent") (collectively the "Asserted Patents") against Zoho Corporation Pvt. Ltd. and Zoho Corporation (collectively "ZOHO" or "Counter-Defendants") and as follows upon actual knowledge with respect to itself and its own acts, and upon information and belief as to all other matters:

I.
PARTIES

1. Liberty Peak Ventures, LLC ("LPV") is a limited liability company with its principal place of business in Allen, Texas.

2. Zoho Corporation Pvt. Ltd is a corporation organized and existing under the laws of the country of India, with a principal place of business at Estancia IT Park, Plot Nos. 140 & 151, GST Road, Vallancherry Village, Chengalpattu Taluk, Kanchipuram District 603 202, India, and is the parent of Zoho Corporation, a wholly owned subsidiary.

3. Zoho Corporation is a California corporation with its headquarters located at 4708 HWY 71 E., Del Valle, TX 78617. Zoho Corporation may be served via its registered agent, Rodrigov Vaca at 9390 Research Blvd, Building II, Suite 440, Austin, Texas 78759.

II.
JURISDICTION AND VENUE

4. The Court has federal question jurisdiction under 28 U.S.C. §§ 1331, and 1338(a) because the action arises under the patent laws of the United States, 35 U.S.C. §§ 271 et seq.

5. On information and belief, venue is proper in this District under 28 U.S.C. § 1400(b) because acts of infringement are occurring in this District and Counter-Defendant Zoho Corporation has over 100 employees at its U.S. Headquarters at 4708 HWY 71 E., Del Valle, TX 78617 whose job functions range from sales and marketing to development and design. As such,

Counter-Defendants have a regular and established place of business in this District and is deemed to be a resident of this District.

6. Venue is proper under 28 U.S.C. § 1391(c)(3) and *In re HTC Corp.*, 889 F.3d 1349 (Fed. Cir. 2018) because Third-Party Defendant Zoho Corporation Pvt. Ltd is a foreign corporation. On information and belief, Zoho Corporation Pvt. Ltd. operates in agency with others, including its U.S. subsidiary, Zoho Corporation, to provide a distribution channel of infringing products within this District and the U.S. nationally. Zoho Corporation Pvt. Ltd., itself and between and amongst its agents and foreign and U.S.-based subsidiaries, purposefully direct the Accused Products into established distribution channels within this District and the U.S. nationally. Zoho Corporation Pvt. Ltd. maintains a corporate presence in the United States through Zoho Corporation and its United States office located within this District.

7. On information and belief, Zoho Corporation Pvt. Ltd. and its U.S.-based sales subsidiaries, including Zoho Corporation (which act as part of a global network of overseas sales and manufacturing subsidiaries on behalf of Zoho Corporation Pvt. Ltd.) have operated as agents of one another and vicariously as parts of the same business group to work in concert together and enter into agreements that are nearer than arm's length. For example, Zoho Corporation Pvt. Ltd., alone and via at least the activities of its U.S.-based sales subsidiaries (e.g., Zoho Corporation), conducts business in the United States, including importing, distributing, and selling the Accused Products that infringe the Asserted Patents in Texas and this judicial district. *See Trois v. Apple Tree Auction Center, Inc.*, 882 F.3d 485, 490 (5th Cir. 2018) ("A defendant may be subject to personal jurisdiction because of the activities of its agent within the forum state…."); *see also Cephalon, Inc. v. Watson Pharmaceuticals, Inc.*, 629 F. Supp. 2d 338, 348 (D. Del. 2009) ("The agency theory may be applied not only to parents and subsidiaries, but also to companies that are

'two arms of the same business group,' operate in concert with each other, and enter into agreements with each other that are nearer than arm's length.").

8. This Court has personal jurisdiction over Counter-Defendants because Counter-Defendants have purposefully availed themselves of the privileges of conducting business in the State of Texas, including through the use, sale and offer for sale of infringing products throughout the State of Texas and this Judicial District. Furthermore, Counter-Defendants have availed themselves of, sought the protection of, and submitted to the jurisdiction of this Court by filing the instant lawsuit against LPV.

9. Counter-Defendants have continuous and systematic business contacts with the State of Texas. Counter-Defendants directly conduct business extensively throughout Texas, by shipping distributing, making, using, offering for sale, selling, licensing, transmitting (including through its website and mobile applications) its products and services in the state of Texas and the Western District of Texas. Counter-Defendants have purposefully placed their products into the stream of commerce with the intention and expectation that they will be purchased and used by consumers in this state and this district. Counter-Defendants have used and continue to use and sell its infringing products within this district and have committed regular acts of direct infringement in this district. Counter-Defendants' contacts with the State of Texas and this district are so pervasive such that this Court's exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

III.
FACTS

10. The Asserted Patents claim inventions born from the ingenuity of the American Express Company ("American Express") and originally developed as part of American Express's digital transaction security technology portfolio. Founded in 1850 as a freight forwarding

company, American Express has been a leader in transaction security for over 170 years.[1] Its business was founded in protecting the national transmission of mail and freight and expanded into financial transactions in 1857.[2] It led the industry in protecting and facilitating international transactions by developing the first Travelers Cheques in 1891.[3]

11. In 1997, American Express introduced its first online business, AXI (American Express Interactive), which served as an e-commerce travel hub.[4] By 1999, American Express had launched several other e-business products providing a variety of financial and business administrative services.[5]

12. Over the past 20 years, the use of electronic and online transactions has grown exponentially. From just 2015 to 2018, the number of remote card transactions grew 20.5 % per year.[6] In 2017, consumers in the U.S. engaged in over 20 Billion remote card transactions with a value totaling over $2.5 Trillion.[7] In 2018, the value of remote card transactions reached $3.29 trillion.[8] And since the COVID-19 pandemic, the public is now more likely to use online forms of ordering and payment going forward.[9] Surveys have reported that consumers are 12% more likely to use online or app-based payments for delivery services, 16% for curbside pickup, and 6% for in-store pickup transactions.[10] In May of 2020, the total U.S. online spending increased by 77% reaching $82.5 billion. [11]

---

[1] https://about.americanexpress.com/our-history/
[2] *Id.*
[3] *Id.*
[4] https://news.microsoft.com/1997/07/14/american-express-and-microsoft-unveil-online-travel-reservations-system-for-corporations/; https://www.businesstravelnews.com/More-News/AXI-Hits-Open-Market
[5] https://sec.report/Document/0000004962-00-000024/
[6] https://www.federalreserve.gov/newsevents/pressreleases/files/2019-payments-study-20191219.pdf
[7] https://www.federalreserve.gov/paymentsystems/2018-December-The-Federal-Reserve-Payments-Study.htm
[8] https://www.federalreserve.gov/newsevents/pressreleases/files/2019-payments-study-20191219.pdf
[9] https://thefintechtimes.com/the-growth-of-contactless-payments-during-the-covid-19-pandemic/; https://www.paymentsjournal.com/contactless-and-covid-19/; https://www.ft.com/content/d56bdbbb-f7f3-4b44-98c3-e1a372ed2280
[10] https://www.cnbc.com/select/contactless-payments-coronavirus/
[11] https://www.ft.com/content/d56bdbbb-f7f3-4b44-98c3-e1a372ed2280

13. This unprecedented move to electronic transactions has also led to a concurrent vulnerability of sensitive consumer information entered, maintained and transmitted by electronic means to attack and theft by malicious actors. In 2019, 42% of consumers reported having been the victim of fraudulent attempts to use their credit card or other payment information.[12] In addition, consumer confidence that businesses are adequately securing their information is trending downward.[13] According to survey results, consumers are eager to have payment information available when they check-out online but are skeptical about the security of maintaining their card on file.[14]

14. To combat this growing malfeasance, American Express was a founding member and developer of the Payment Card Industry Data Security Standards (PCI DSS) in December 2004, which required all merchants to adopt a common set of security standards to combat fraud in merchant transactions.[15] In addition to these efforts, American Express developed the technology embodied by the Asserted Patents to protect sensitive customer information from attack and theft.

A. Nature of The Action

15. LPV is the owner by assignment of all right, title and interest in and to the ’122 Patent, the ’088 Patent, and the ’901 Patent.

16. This is an action for direct patent infringement.

17. LPV alleges that Counter-Defendants have directly infringed and continue to directly infringe, the ’122 Patent, the ’088 Patent, and the ’901 Patent.

---

[12] https://network.americanexpress.com/globalnetwork/dam/jcr:09c34553-b4a2-43ca-bf3e-47cbc911ea51/American%20Express%202019%20Digital%20Payments%20Survey_Insights%20Paper.pdf
[13] *Id.*
[14] *Id.*
[15] https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard.

18. A true and correct copy of the '122 Patent is attached as Exhibit A to this Complaint.

19. The U.S. Patent and Trademark Office ("USPTO") granted the '122 Patent on June 21, 2016, after a full and fair examination.

20. The '122 Patent is valid and enforceable.

21. A true and correct copy of the '088 Patent is attached as Exhibit B to this Complaint.

22. The U.S. Patent and Trademark Office ("USPTO") granted the '088 Patent on September 11, 2018 after a full and fair examination.

23. The '088 Patent is valid and enforceable.

24. A true and correct copy of the '901 Patent is attached as Exhibit C to this Complaint.

25. The U.S. Patent and Trademark Office ("USPTO") granted the '901 Patent on March 23, 2021 after a full and fair examination.

26. The '901 Patent is valid and enforceable.

1. The '122 Patent

27. The '122 Patent relates generally to the field of security in the maintaining and processing of customer account data, and more particularly, to systems, computer programs, and methods for securing databases and securely interfacing with secured databases containing sensitive account information with a client system tool.

28. The '122 Patent is directed to solving problems particular to the transmission of sensitive customer account data to a computing device such that the data is not exposed to malicious entities external or internal to the computing device. Solutions provided in embodiments of the '122 Patent provide methods for storing and securing sensitive information using secure remote and/or segregated storage of encrypted data where decryption of the data is provided at a

local toolbar using an encryption key.

29. At the time that the application leading to the '122 Patent was filed, the proliferation of rogue programs such as viruses, trojan horses, and computer hackers, etc., placed computing devices at risk. This risk extended to customer account data, which even stored temporarily was potentially vulnerable to malicious entities. As a result, customers, merchants, and card issuers were reluctant to utilize tools that resided on a customer computing device and interface with customer account data.

30. Yet, at the time, online shopping through customer computing devices was becoming as common as in-store shopping. Remote payment transactions are typically performed by a customer through a personal computer connected to a public network such as the Internet. Typically, a customer, whether through the merchant's website or a third-party payment processing website, manually entered his or her account information into fields on a web page to process a transaction.

31. To avoid memorizing information, such as account numbers, and to avoid typing additional information used to make a purchase, some customers used account storage data programs allowing customers to avoid the tedious task of manually entering this information during each transaction. These programs or devices are often referred to as "digital wallet" or "e-wallet" programs.

32. One drawback of prior art digital wallet programs was that information that was automatically or manually loaded into a customer's device could still be exposed to rogue programs running on the customer's computing device. Thus, even if the account data was stored in an encrypted form, the account data could be exposed at the point of entry or prior to encryption by the digital wallet.

33. Another failing of prior art digital wallet programs was that customer account information that was transmitted from a remote database to a customer's device could also be potentially accessed by malicious entities once it was decrypted on the customer's device (e.g., where the information may have been stored encrypted, but was transmitted once it was decrypted on the customer's device, or where a customer was sent a key). As a result, card issuers (or those maintaining sensitive customer account information) were reluctant to provide customer computing devices access to customer account data, and typically limited access to such data. For example, while customers were able to access recent transactions, payments, and statement through card issuer websites, the interfaces did not provide access to account data necessary for actual transaction processing.

34. The shortcomings of the prior art digital wallet conventional prior art were solved by the unconventional and inventive system, methods, and devices claimed by the '122 patent.

35. Claim 1 of the '122 Patent covers "a method comprising (a) detecting, at a browser toolbar of a computer system, a request from a web service to obtain account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder; (b) sending, by the browser toolbar, a request for the account information to a secure database that stores the account information; (c) decrypting, by the browser toolbar, encrypted data received from the secure database, wherein the encrypted data includes the account information, wherein the decrypting is performed using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar; (d) securely storing the account information at the browser toolbar; and (e) removing the stored account information from the browser toolbar after completion of the transaction.

36. Claim 8 of the '122 Patent covers "a system comprising: (a) a processor; (b)

memory having instructions stored therein that are executable by the processor to implement a browser toolbar that performs; (i) identifying a request from a web service for account information associated with an account holder, wherein the account information is usable to conduct a transaction with the account holder; (ii) retrieving an encrypted version of the account information from the remote database; (iii) decrypting the encrypted version of the account information using the encryption key maintained by the browser toolbar; (iv) completing a website form of the web service with a decrypted version of account information; and (v) deleting the decrypted version of the account information after completing the website form."

37. A person of ordinary skill in the art at the time of the invention would recognize that the steps, methods, and devices claimed by the '122 Patent were unconventional and describe identifying a request from a web service for account information that is associated with an account holder and then decrypting, and then deleting the decrypted version of, the account information after completing the website form.

38. A person of ordinary skill in the art at the time of the invention of the '122 Patent would understand that the conventional way of completing online transactions were vulnerable to malicious intervention due to the accessibility of unencrypted account information at various points throughout the transaction. A skilled artisan would recognize that the conventional methods of inputting unencrypted sensitive account information, whether by the account holder or remote agent, presented the problems of simultaneously granting access to unencrypted account information outside of the program conducting the transaction, outside the specific transaction itself, and/or allowed the information to persist in memory.

39. The '122 Patent solves all of these vulnerabilities simultaneously and improves the functionality of the online transaction methods, systems, and devices themselves. This is

accomplished in at least one embodiment by detecting, at a browser toolbar of a computer system, a request from a web service to obtain account information. A request is also sent for account information to a secure database that stores account information and the encrypted data received from this database is decrypted using an encryption key maintained by the browser toolbar. This account information is stored securely at the browser toolbar and then removed after the completion of the transaction. The unencrypted information is not persistent in memory and therefore not available outside of the toolbar or the transaction.

40. A person skilled in the art at the time of the invention of the '122 Patent would understand the claims, including at least Claim 1, recite an ordered combination of steps operating in an unconventional manner to achieve an improved method of securing account information during the completion of online transactions.

41. These technological improvements provide the advantages of: (1) a secure method of completing online transactions; (2) protecting sensitive account information within the confines of an individual transaction; (3) protecting sensitive account information within the confines of a browser toolbar; (4) providing remote secure storage of sensitive account information; (5) providing local decryption at a browser toolbar; (6) protecting sensitive account information from snooping during input of such information; (7) ameliorating the vulnerability associated with storing sensitive account information persistently in memory; (8) encrypting sensitive account information at all times outside of an individual transaction and a browser toolbar; and (9) removing the need to manually input sensitive account information.

42. The novel use and arrangement of the specific combination, steps, system, and devices recited by the '122 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions. In particular, the ordered combination of

steps in at least Claim 1 of the '122 Patent were not well understood, routine, or conventional to a person of skill in the relevant field at the time of the inventions, particularly, the steps of decrypting, by the browser toolbar, encrypted data received from the secure database, wherein the decrypting is performed using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar; securely storing the account information at the browser toolbar; and removing the stored account information from the browser toolbar after completion of the transaction, were not well-understood, routine or conventional to a person of skill in the relevant field at the time of the invention.

43. The '122 Patent claims a novel architecture for systems that manage sensitive data. The '122 Patent appends the traditional, e.g., password management system architecture by separating the storage of sensitive information from the locale where that information is encrypted/decrypted. This architecture provides a technical solution to problems related to utilizing tools that reside on a customer computing device and interface with customer account data; it affords the resilience and convenience of remote storage, while benefiting from the enhanced security of local encryption and decryption of user data.

2. The '088 Patent

44. The '088 Patent relates generally to the field of security in the maintaining and processing of customer account data, and more particularly, to systems, computer programs, and methods for securing databases and securely interfacing with secured databases containing sensitive account information with a client system tool.

45. The '088 Patent is directed to solving problems particular to the transmission of encrypted sensitive customer account data to a computing device such that the data is not exposed to malicious entities external or internal to the computing device. Solutions provided in

embodiments of the ’088 Patent provide methods for storing and securing sensitive information using secure database storage of encrypted data where decryption of the data is provided at a local toolbar using an encryption key.

46. Claim 1 of the ’088 Patent covers “a method comprising (a) generating, at a browser toolbar, a cryptographic key, usable to decrypt encrypted account information of an account holder, wherein the account information is useable to conduct a transaction with the account holder; (b) sending, by the browser toolbar, a request for the account information to a secure database that stores the account information; (b) using, by the browser toolbar, the cryptographic key to decrypt data received from the secure database, wherein the encrypted data includes the account information; (c) securely storing, by the browser toolbar, the account information at the browser toolbar, and (d) providing, by the browser toolbar, the account information to a web service in response to a request.”

47. Claim 2 of the ’088 Patent covers the “method of Claim 1, wherein the generating further comprises (a) generating a public key pair having a public key and private key, wherein the private key is the cryptographic key; and (b) transmitting the public key to the secure database for encrypting the account information.”

48. A person of ordinary skill in the art at the time of the invention would recognize that the steps and methods claims in at least Claims 1 and 2 of the ’088 Patent were unconventional and describe generating a cryptographic key at a browser toolbar, usable to decrypt encrypted account information of an account holder, using, by the browser toolbar, the cryptographic key to decrypted to decrypt the account information while securely storing the account information at the browser toolbar and providing the account information to a web service in response to a request.

49. A person of ordinary skill in the art at the time of the invention of the ’088 Patent

would understand that the conventional way of completing online transactions were vulnerable to malicious intervention due to the accessibility of unencrypted account information at various points throughout the transaction. A skilled artisan would recognize that the conventional methods of inputting unencrypted sensitive account information, whether by the account holder or remote agent, presented the problems of simultaneously granting access to unencrypted account information outside of the program conducting the transaction, outside the specific transaction itself, and/or allowed the information to persist in memory.

50. The ’088 Patent solves all of these vulnerabilities simultaneously and improves the functionality of the online transaction methods, systems, and devices themselves. This is accomplished by, in at least one embodiment, by generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder. A request is also sent for account information to a secure database that stores account information and using by the browser toolbar, the cryptographic key to decrypt data received from the secure database. The account information is stored securely by and at the browser toolbar and sent to a web service in response to a request. The unencrypted information is not persistent in memory and therefore not available outside of the toolbar or the transaction.

51. A person skilled in the art at the time of the invention of the ’088 Patent would understand the claims, including at least Claims 1 and 2, recited an ordered combination of steps operating in an unconventional manner to achieve an improved method of securing account information during the completion of online transactions.

52. These technological improvements provide the advantages of: (1) a secure method of completing online transactions; (2) providing remote secure storage of sensitive account information; (3) providing local decryption at a browser toolbar; (4) generating, at an account

toolbar, a cryptographic public key pair for encrypting and decrypting sensitive information; (4) decrypting sensitive account information at all times inside of a browser toolbar; and (5) removing the need to manually input sensitive account information.

53. The novel use and arrangement of the specific combination, steps, system, and devices recited by the '088 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions. In particular, the ordered combination of steps in at least Claim 1 and 2 of the '088 Patent were not well understood, routine, or conventional to a person of skill in the relevant field at the time of the inventions, particularly, the steps of generating, at a browser toolbar, a cryptographic key, usable to decrypt encrypted account information of an account holder, wherein the account information is useable to conduct a transaction with the account holder; using, by the browser toolbar, the cryptographic key to decrypt data received from the secure database, wherein the encrypted data includes the account information; and securely storing, by the browser toolbar, the account information at the browser toolbar, were not well-understood, routine or conventional to a person of skill in the relevant field at the time of the invention.

54. The '088 Patent claims a novel architecture for systems that manage sensitive data. The '088 Patent appends the traditional, e.g., password management system architecture by separating the storage of sensitive information from the locale where that information is encrypted/decrypted. This architecture provides a technical solution to problems related to utilizing tools that reside on a customer computing device and interface with customer account data; it affords the resilience and convenience of remote storage, while benefiting from the enhanced security of local encryption and decryption of user data.

3. The ’901 Patent

55. The ’901 Patent relates generally to the field of security in the maintaining and processing of customer account data, and more particularly, to systems, computer programs, and methods for securing databases and securely interfacing with secured databases containing sensitive account information with a client system tool.

56. The ’901 Patent is directed to solving problems particular to the transmission of encrypted sensitive customer account data to a computing device such that the data is not exposed to malicious entities external or internal to the computing device. Solutions provided in embodiments of the ’901 Patent provide methods for storing and securing sensitive information using secure storage of encrypted data where decryption of the data by a toolbar uses an encryption key.

57. Claim 1 of the ’901 Patent covers a method, comprising: (a) generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder; (b) detecting, by the browser toolbar, a first request to obtain the account information of the account holder; (c) sending, by the browser toolbar, a second request for the account information to a secure datastore that stores the account information; (d) using, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure datastore, wherein the encrypted data includes the account information; (e) securely storing, by the browser toolbar, the account information at the browser toolbar; and providing, by the browser toolbar, the account information to a web service in response to the first request.

58. A person of ordinary skill in the art at the time of the invention would recognize that the steps and methods claimed by at least Claim 1 of the ’901 Patent were unconventional and

describe generating a cryptographic key usable to decrypt encrypted account information of an account holder, detecting a first request to obtain account information of the account holder, sending, by the browser toolbar, a second request for the account information to a secure datastore, using, by the browser toolbar, the cryptographic key to decrypt the encrypted data received from the secure datastore, and securely storing the account information at the browser toolbar and providing the account information to a web service in response to a request.

59. A person of ordinary skill in the art at the time of the invention of the '901 Patent would understand that the conventional way of completing online transactions were vulnerable to malicious intervention due to the accessibility of unencrypted account information at various points throughout the transaction. A skilled artisan would recognize that the conventional methods of inputting unencrypted sensitive account information, whether by the account holder or remote agent, presented the problems of simultaneously granting access to unencrypted account information outside of the program conducting the transaction, outside the specific transaction itself, and/or allowed the information to persist in memory.

60. The '901 Patent solves all of these vulnerabilities simultaneously and improves the functionality of the online transaction methods, systems, and devices themselves. This is accomplished by, in at least one embodiment, by generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder. A request is also sent for account information to a secure datastore that stores account information and using by the browser toolbar, the cryptographic key to decrypt data received from the secure datastore. The account information is stored securely by and at the browser toolbar and sent to a web service in response to a request. The unencrypted information is not persistent in memory and therefore not available outside of the toolbar or the transaction.

61. A person skilled in the art at the time of the invention of the '901 Patent would understand the claims, including at least Claim 1, recited an ordered combination of steps operating in an unconventional manner to achieve an improved method of securing account information during the completion of online transactions.

62. These technological improvements provide the advantages of: (1) a secure method of completing online transactions; (2) providing remote secure storage of sensitive account information; (3) providing local decryption at a browser toolbar; (4) detecting, by the browser toolbar, a request for account information; (5) decrypting sensitive account information at all times inside of a browser toolbar; and (6) removing the need to manually input sensitive account information or determine where on a website such information needed to be input.

63. The novel use and arrangement of the specific combination, steps, system, and devices recited by the '901 Patent were not well-understood, routine, or conventional to a person skilled in the relevant field at the time of the inventions. In particular, the ordered combination of steps in at least Claim 1 of the '901 Patent were not well understood, routine, or conventional to a person of skill in the relevant field at the time of the inventions, particularly, the steps of generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder; detecting, by the browser toolbar, a first request to obtain the account information of the account holder; sending, by the browser toolbar, a second request for the account information to a secure datastore that stores the account information; using, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure datastore, wherein the encrypted data includes the account information; securely storing, by the browser toolbar, the account information at the browser toolbar; and providing, by the browser

toolbar, the account information to a web service in response to the first request toolbar, were not well-understood, routine or conventional to a person of skill in the relevant field at the time of the invention.

64. The ’901 Patent claims a novel architecture for systems that manage sensitive data. The ’901 Patent appends the traditional, e.g., password management system architecture by separating the storage of sensitive information from the locale where that information is encrypted/decrypted. This architecture provides a technical solution to problems related to utilizing tools that reside on a customer computing device and interface with customer account data; it affords the resilience and convenience of remote storage, while benefiting from the enhanced security of local encryption and decryption of user data.

B. The Accused Products

65. Counter-Defendants offer a suite of software applications operable across several computing platforms including, at least, its Zoho Vault password managing application (“Vault”). Zoho offers their password managing service through stand-alone software applications, mobile applications, and browser extensions for Chrome, Firefox, Edge, Safari, Vivaldi, and Brave. Zoho’s password management services are offered for operating programs including iOS, Windows, and Android.

66. Zoho’s Vault application is advertised as being able to protect a user’s passwords and sensitive information through vault encrypted databases, manage the user’s passwords, share a single user’s information across platforms, and securely share information among multiple users through the webservice. The application manages user passwords and “auto-fills” them across websites and applications and allows for sharing a user’s information across platforms. The application also provides for securely sharing information among multiple users through the web

service. Through their Vault application, Counter-Defendants offer its account holders an electronic "vault" in which a user is able to store the user's passwords for various accounts and payment methods, payment information, banking information, sensitive documents, and other information as "secrets" as well as create and use virtual payment cards.

67. Through Zoho's Vault application, Counter-Defendants provide a password managing service through which a user is able to access, transfer, and provide secure information across various platforms by simply using one "master" password. This is a prominent feature advertised by Counter-Defendants. In conjunction with this functionality, Vault includes an "auto-fill" feature that detects, and places certain stored sensitive user information into forms used to access websites and participate in online transactions.

68. Counter-Defendants advertise that its data security is achieved through "host-proof-hosting" using RSA encryption and cryptographic keys. The data stored and protected on the system are both encrypted and decrypted through a two-secret key derivation. This is achieved by using a unique password identified as the "master password". The master password is used to protect the data stored on a user's device. The user then creates a key, which when used with the master password allows Counter-Defendants to encrypt the data. Counter-Defendants advertise that all user data "gets encrypted and decrypted in the browser with the user's Zoho Vault master password, and only the encrypted data gets stored in Zoho's servers. The user's master password is never stored anywhere by Zoho Vault".

69. Counter-Defendants further advertise that all encryption and decryption takes place in the client side (browser) and that the information stored in its vault is encrypted by using Advanced Encryption Standard (AES) using 256-bit keys that are generated on the device. The method used in encrypting and decrypting information is through a public and private key pair,

which are generated using cryptographic keys. Counter-Defendants advertise that all sensitive data, including passwords, are stored in a fully encrypted form. The data is encrypted in the user's browser and then transmitted in a fully encrypted form over SSL. "Our data center holds only your encrypted data."[16]

70. Upon information and belief, due to these and other aspects of the Vault application, Counter-Defendants have and continue to directly infringe the '122 Patent, the '088 Patent, and the '901 Patent as described in the Counts below.

CAUSES OF ACTION
COUNT I: DIRECT INFRINGEMENT OF THE '122 PATENT

71. LPV realleges and incorporates by reference the allegations set forth above as if set forth verbatim herein.

72. LPV owns by assignment the entire right, title, and interest in the '122 Patent, including the right to sue for past infringement.

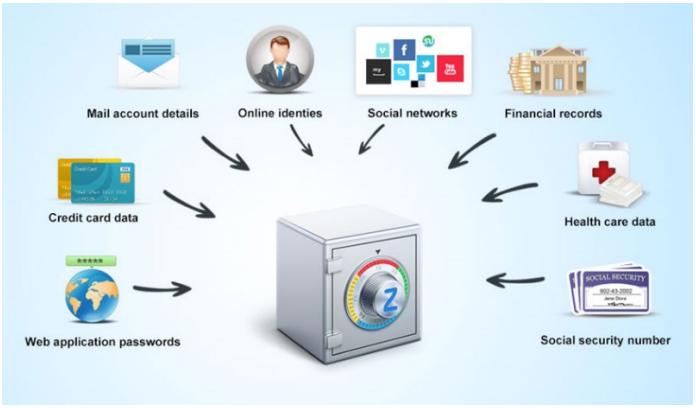
73. The '122 Patent was issued by the United States Patent and Trademark Office on June 21, 2016 and is titled "Methods, Apparatus and Computer Program Products for Securely Accessing Account Data". A true and correct copy of the '122 Patent is attached as Exhibit A.

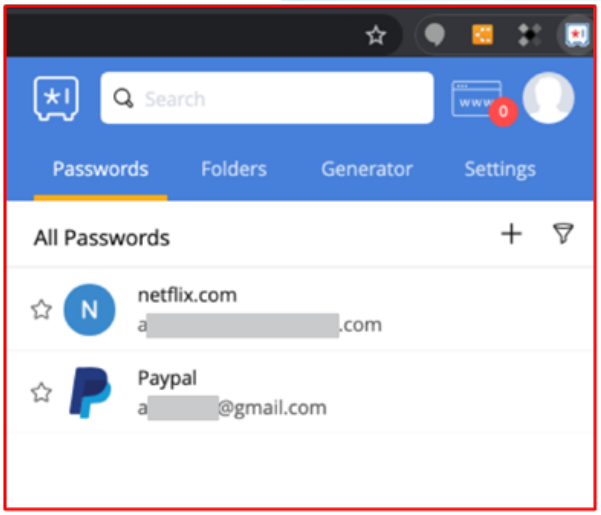
74. Upon information and belief, Counter-Defendants have directly infringed and continue to directly infringe at least Claim 1 of the '122 Patent by making, using, testing (including their own use and testing), selling, offering for sale, importing and/or licensing in the United States without authority systems, products, and methods claimed by the '122 Patent, namely, the Vault application.

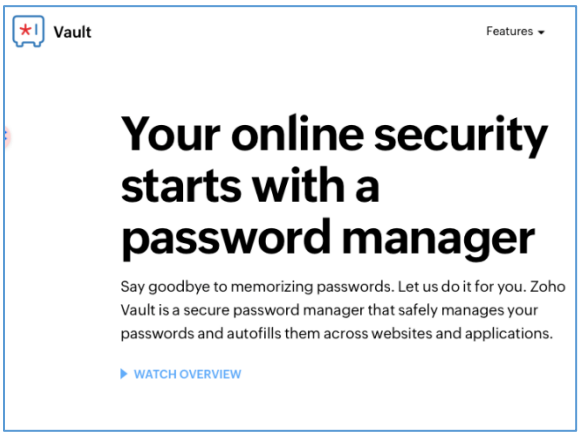
75. Upon information and belief, and as one illustration without limitation, Counter-Defendants infringe Claim 1 of the '122 Patent in the exemplary manners described below.

[16] https://www.zoho.com/vault/help/faq.html#data-security-and-privacy

76. Counter-Defendants' Vault application provides a secure electronic "vault" including a digital wallet that allows users to store passwords and other account information as well as credit card and banking information.







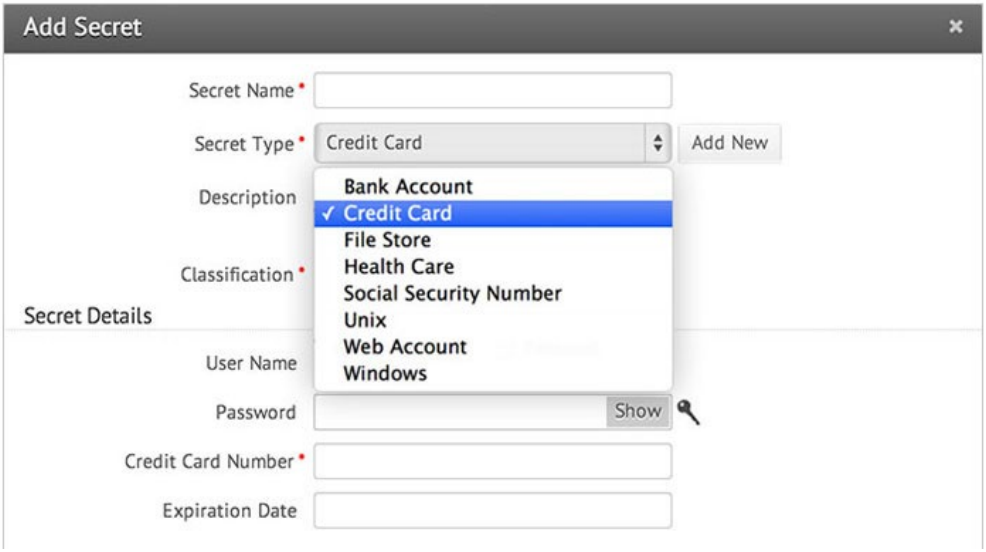


Figure 1[17]

77. Zoho's Vault detects, at a browser toolbar of a computer system, a request from a web service to obtain account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder. For example, the Vault application detects and automatically populates fields on a website with credit card information (i.e., "account information") that are used to conduct, for example, a payment transaction.

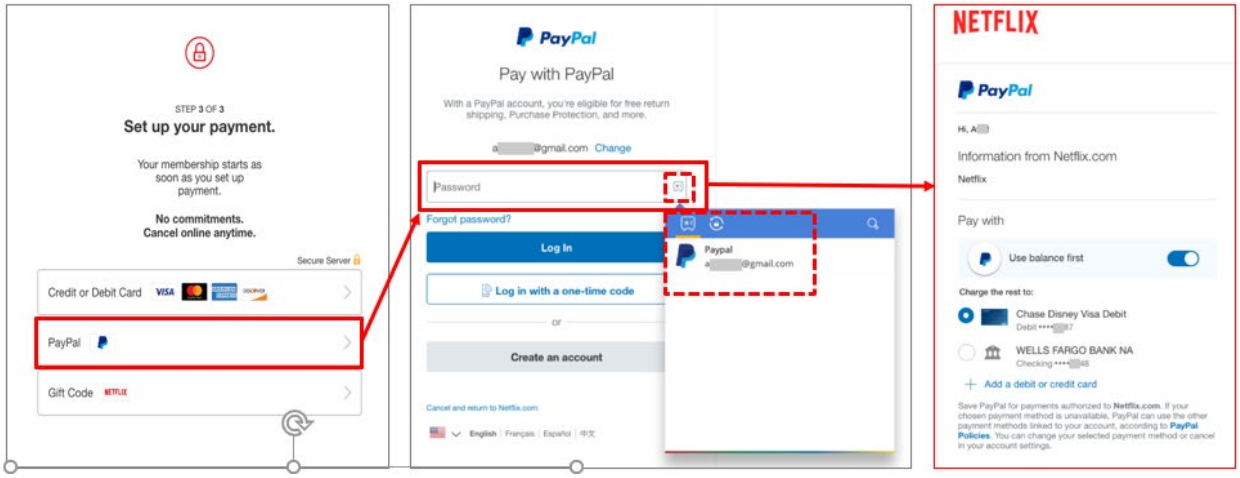


Figure 2[18]

78. The Vault application sends, by the browser toolbar, a request for the account information to a secure database that stores the account information. For example, the Vault application sends a request to access user account information that is stored in a secure database in the cloud in an encrypted form. The Vault application syncs with the cloud server periodically to store a local version of the encrypted data.

[17] https://www.zoho.com/blog/general/introducing-zoho-vault-online-password-manager-for-teams.html; https://www.zoho.com/vault/adding-secrets.html; https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html

[18] Zoho Vault interfaces by a user using a PayPal transaction to obtain a Netflix subscription; *see* https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html; https://help.zoho.com/portal/en/kb/vault/user-guide/articles/vault-auto-log-in-to-websites#Using_the_autofill_icon_from_the_extension

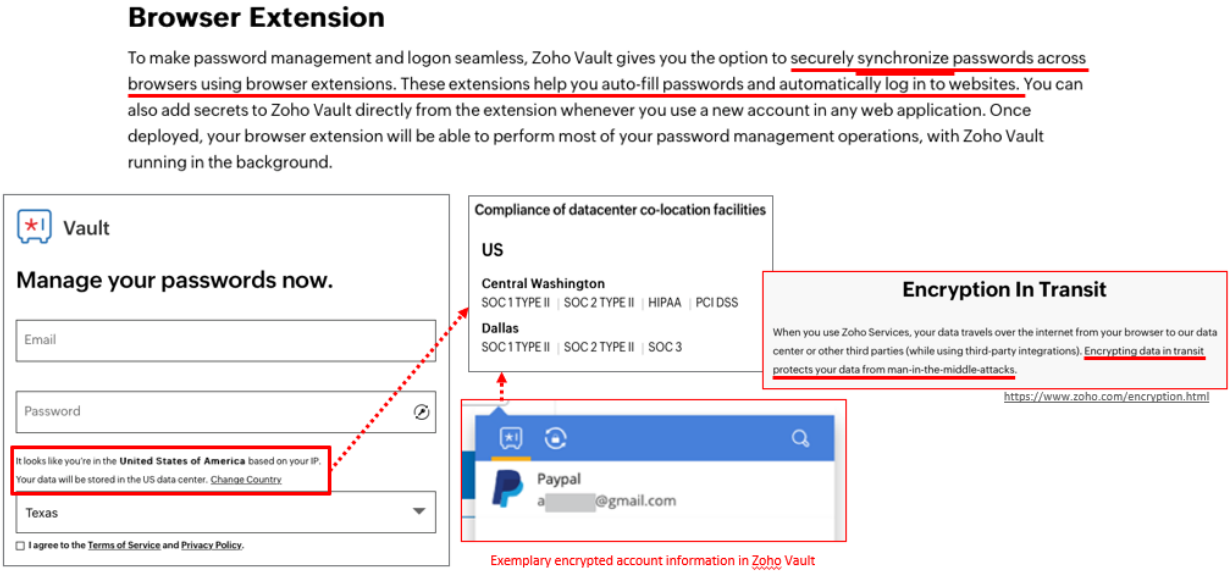


Figure 3[19]

79. The Vault application uses, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure database, wherein the encrypted data includes account information. For example, the Vault application uses a locally generated and stored encryption key to decrypt user account data.

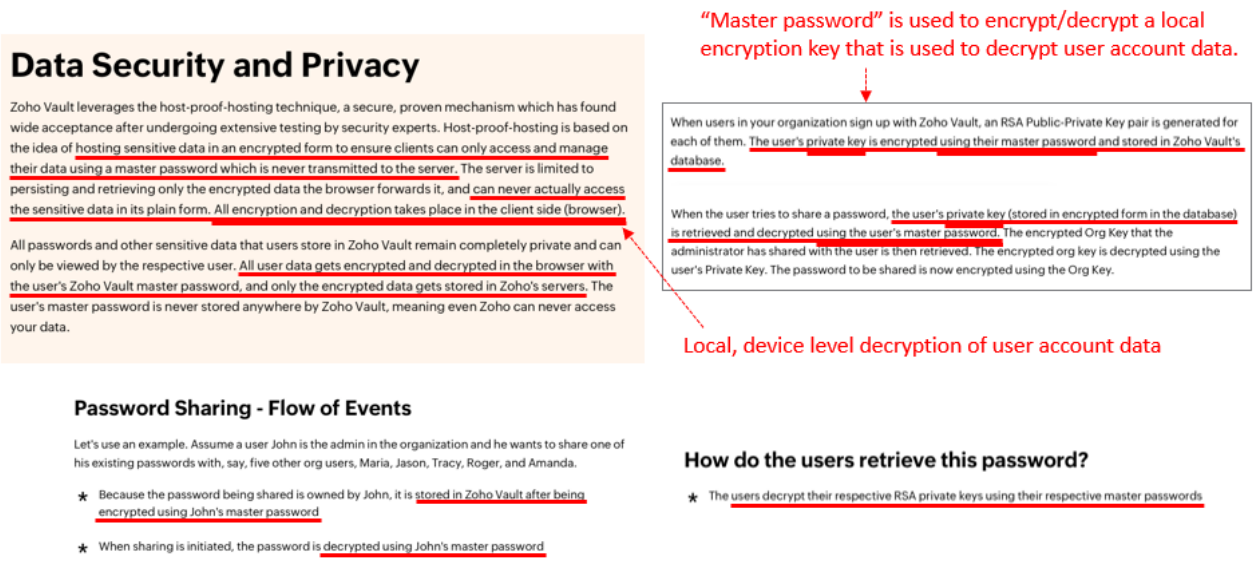


Figure 4[20]

[19] https://www.zoho.com/vault/browser-extension.html; https://www.zoho.com/know-your-datacenter.html; https://www.zoho.com/vault/signup.html; https://www.zoho.com/encryption.html
[20] https://www.zoho.com/vault/security.html

80. The Vault Application securely stores the account information at the browser toolbar. For example, once the Vault application has decrypted the user data, the raw data (i.e., account information) is stored in the temporary memory (RAM) for a limited period of time as a CPU process memory. The decrypted user data is inaccessible outside of the browser toolbar application.

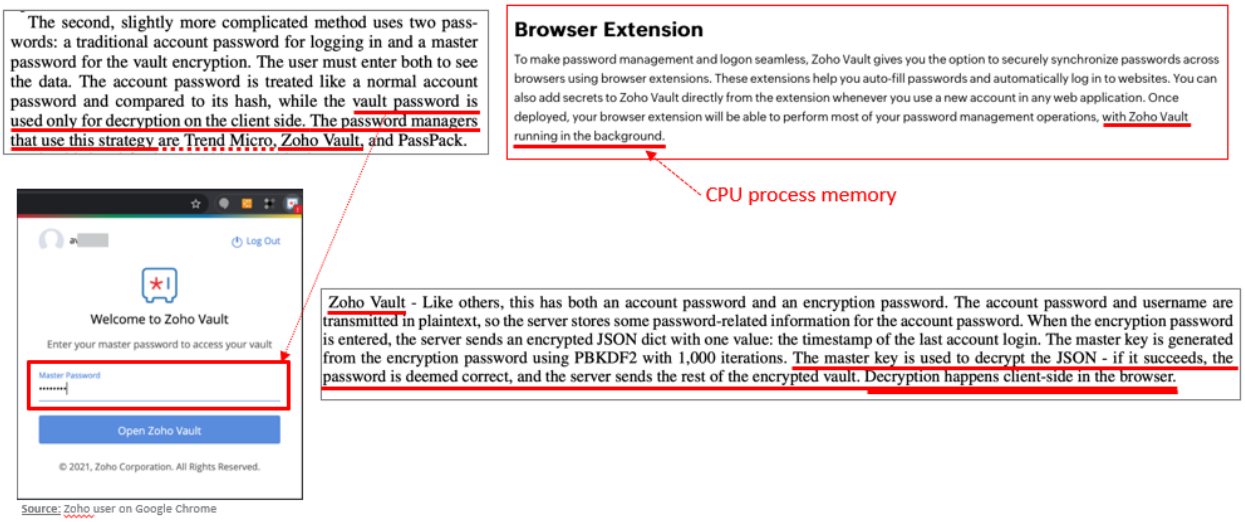


Figure 5[21]

81. The Vault application removes the stored account information from the browser toolbar after completion of the transaction. For example, the raw account information is only available in the Vault application until the transaction is complete, otherwise only the encrypted data is stored.

[21] https://www.zoho.com/vault/browser-extension.html; https://www.osti.gov/servlets/purl/1257179

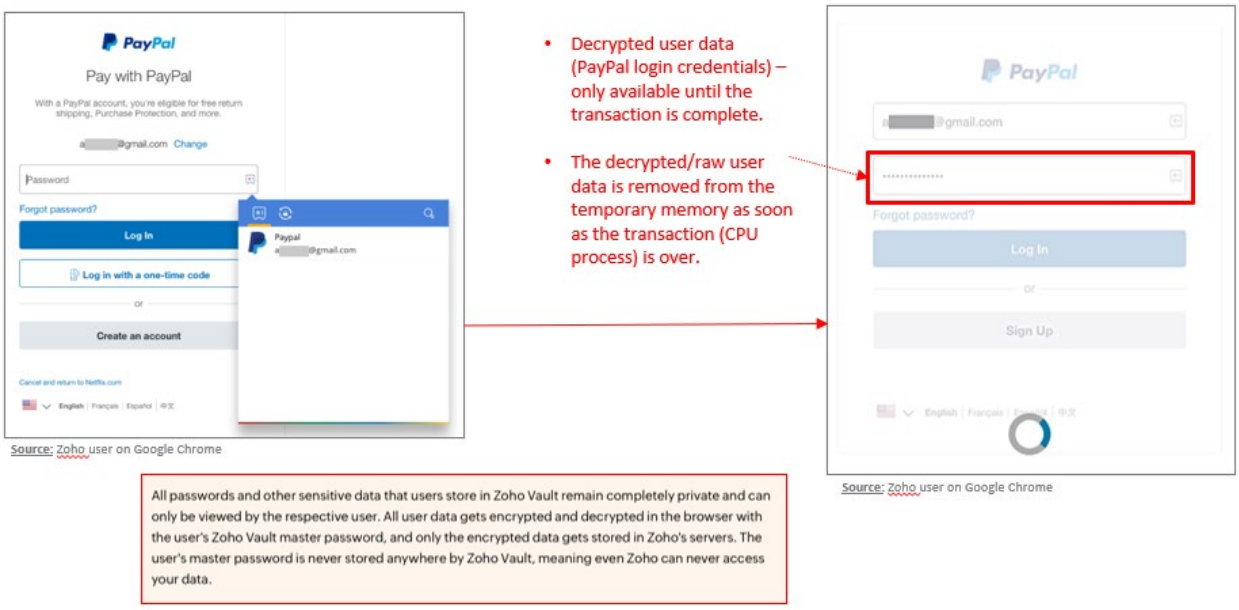


Figure 6[22]

82. To the extent that Counter-Defendants have assigned performance of these steps to third parties, such as its customers, agents or contractors, the third parties act vicariously as agents of the Counter-Defendants, or form a joint enterprise with Counter-Defendants, to infringe at least Claim 1 of the '122 Patent. Alternatively, the Counter-Defendants contract with the third parties to perform the infringing steps. Counter-Defendants profit vicariously from third party infringement, condition the third parties' participation and receipt of benefits of the Vault application on the performance on the infringing activity and further establish the respective timing and manner of the third parties' performance of the infringing activity.

83. Counter-Defendants also form a joint enterprise among themselves, and act vicariously through each other, to infringe at least Claim 1 of the '122 Patent.

84. Counter-Defendants' infringing activities were and are without authority or license under the '122 Patent. Thus, Counter-Defendants have, and continue to infringe at least Claim 1 of the '122 Patent under at least 35 U.S.C. § 271(a) by their continued use, testing, manufacture,

[22] https://www.zoho.com/vault/security.html

sale, offer for sale, licensing, and/or importation of the Accused Products without authority.

COUNT II: DIRECT INFRINGEMENT OF THE '088 PATENT

85. LPV realleges and incorporates by reference the allegations set forth above as if set forth verbatim herein.

86. LPV owns by assignment the entire right, title, and interest in the '088 Patent, including the right to sue for past infringement.

87. The '088 Patent was issued by the United States Patent and Trademark Office on September 11, 2018 and is titled "Methods, Apparatus and computer Program Products for Securely Accessing Account Data." A true and correct copy of the '088 Patent is attached as Exhibit B.

88. Upon information and belief, Counter-Defendants have directly infringed and continue to directly infringe at least Claim 1 of the '088 Patent by making, using, testing (including their own use and testing), selling, offering for sale, importing and/or licensing in the United States without authority systems, products, and methods claimed by the '088 Patent, namely, the Zoho Vault application.

89. Upon information and belief, and as one illustration without limitation, Counter-Defendants infringe Claim 1 of the '088 Patent in the exemplary manner described below.

90. Counter-Defendants' Vault application provides a secure electronic "vault" including a digital wallet that allows users to store passwords and other account information as well as credit card and banking information.

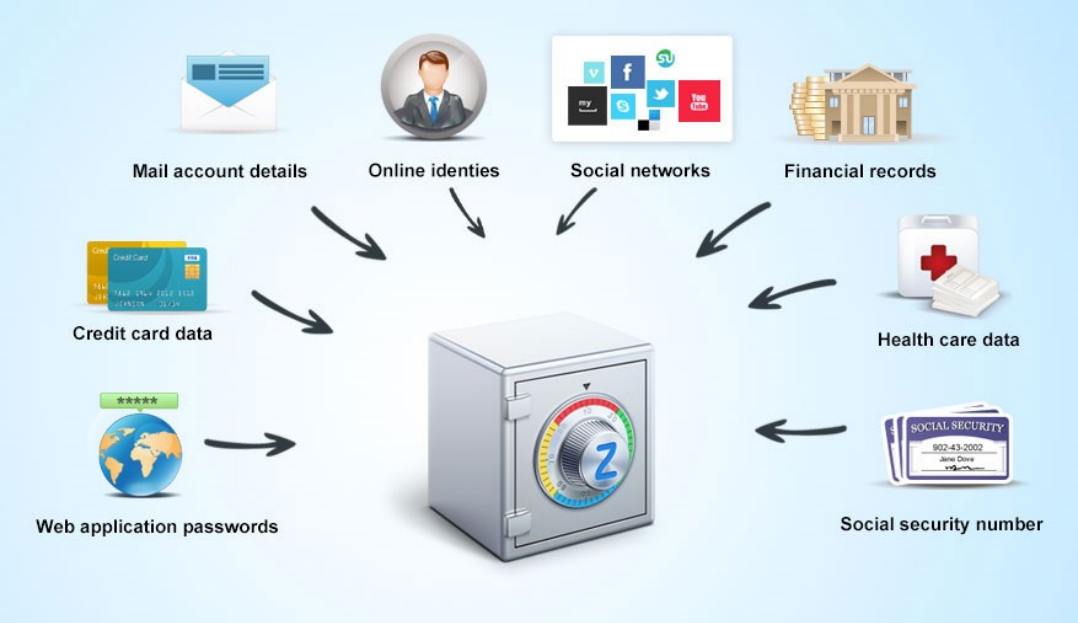


Figure 7[23]

91. The Vault application generates, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder. For example, the Vault application locally generates and stores encryption keys and account information which can then be used to conduct transactions.

[23] https://www.zoho.com/blog/general/introducing-zoho-vault-online-password-manager-for-teams.html

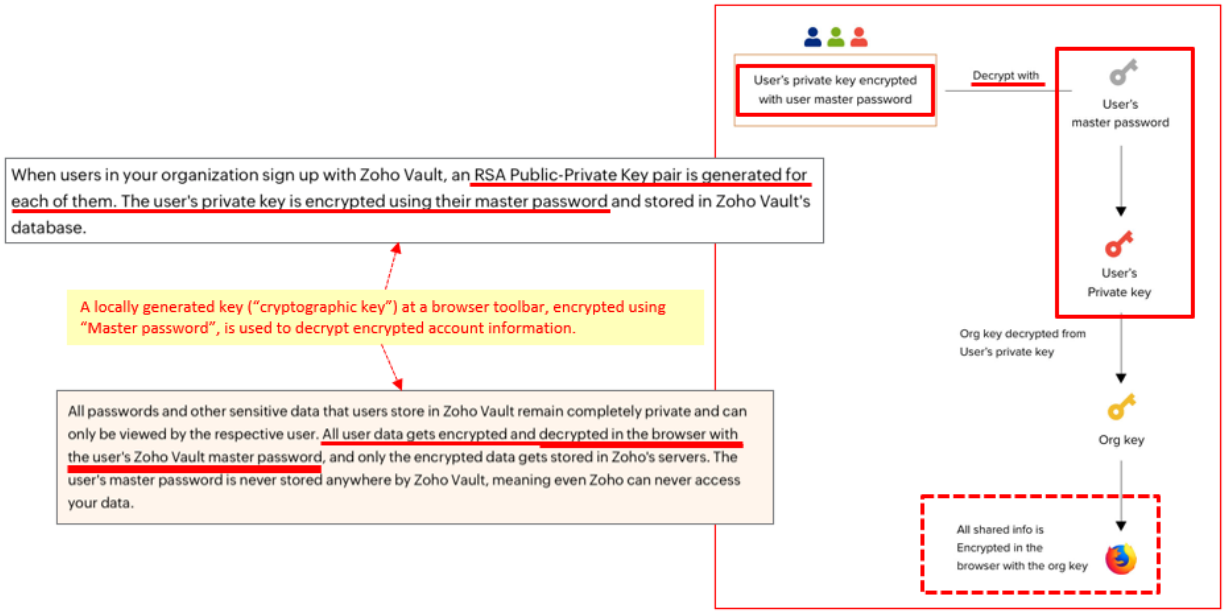


Figure 8[24]

92. The Vault application sends, by the browser toolbar, a request for the account information to a secure database that stores the account information. For example, the Vault application stores the account information securely in the cloud and syncs with the cloud periodically to store a local version of the encrypted data.

[24] https://www.zoho.com/vault/security.html

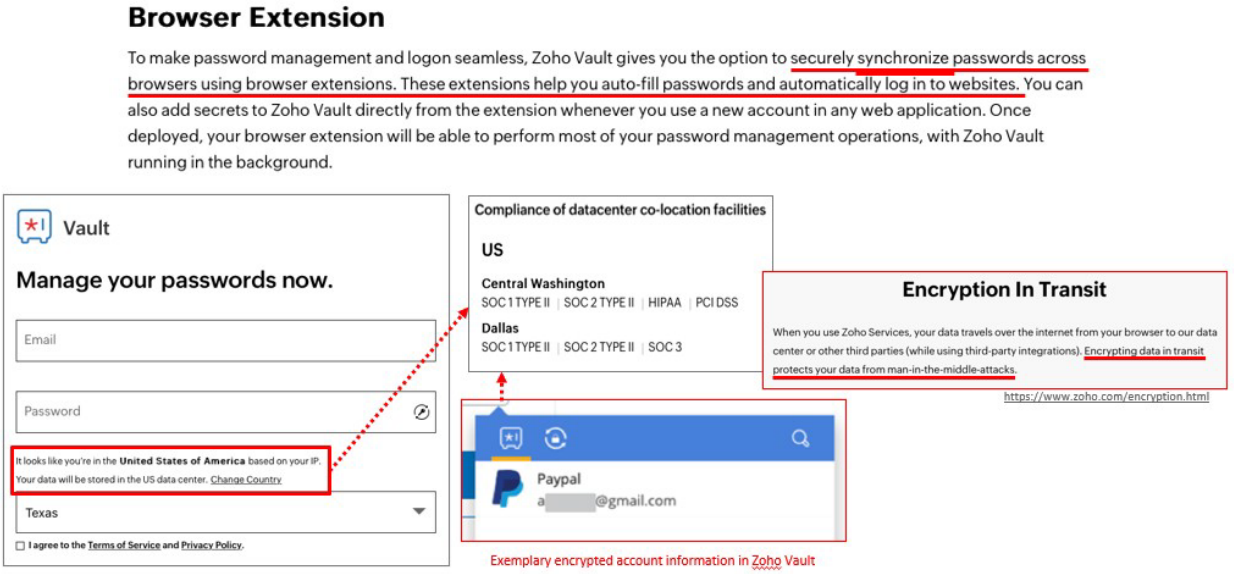


Figure 9[25]

93. The Vault application uses, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure database, wherein the encrypted data includes account information. For example, the Vault application uses the locally generated user encryption key ("cryptographic key") to decrypt user account data.

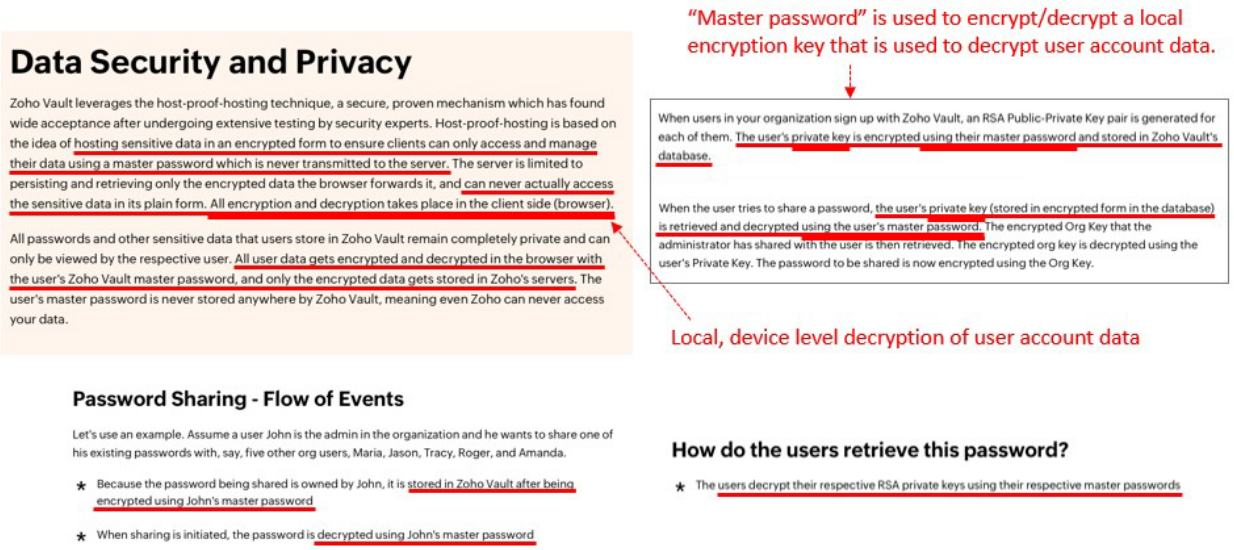


Figure 10[26]

[25] https://www.zoho.com/vault/browser-extension.html; https://www.zoho.com/know-your-datacenter.html; https://www.zoho.com/vault/signup.html; https://www.zoho.com/encryption.html;
[26] https://www.zoho.com/vault/security.html

94. The Vault application securely stores the account information at the browser toolbar. For example, once the Vault application has decrypted user data, the raw data is stored in the temporary memory (RAM) for a limited period of time as a CPU process memory. The decrypted user data is inaccessible outside of the browser toolbar application.

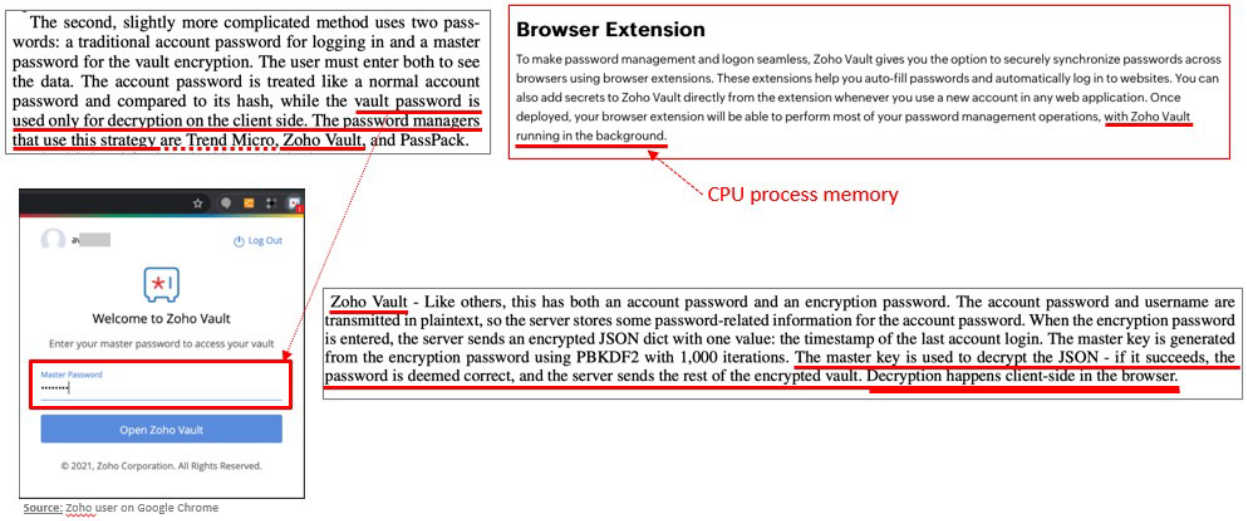


Figure 11[27]

95. The Vault application, provide by the browser toolbar, the account information to a web service in response to a request. For example, the Vault application automatically populates fields on a website with user account information (e.g., PayPal credentials).

[27] https://www.zoho.com/vault/browser-extension.html; https://www.osti.gov/servlets/purl/1257179

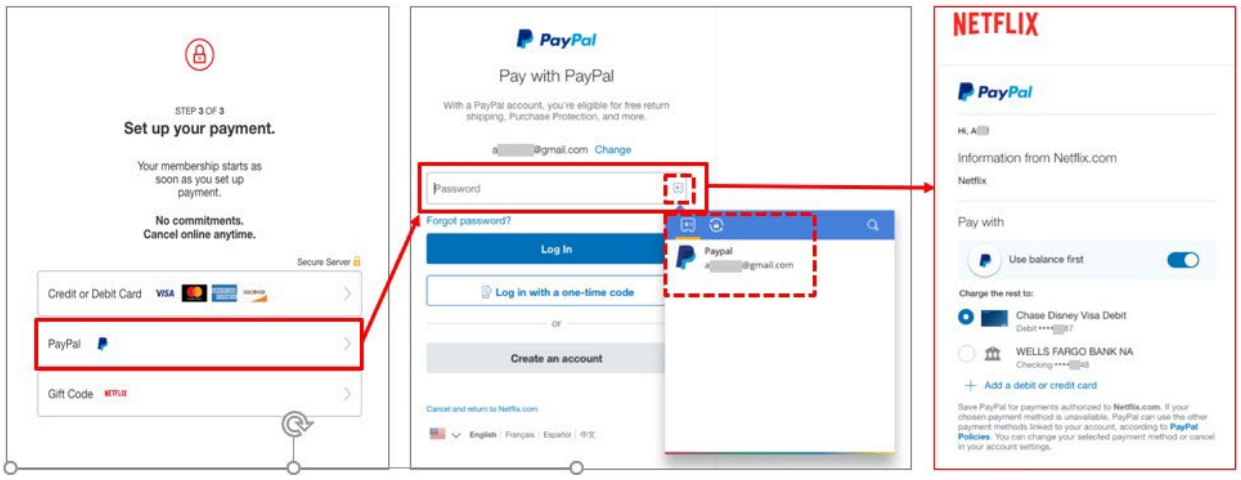


Figure 12[28]

96. To the extent that Counter-Defendants have assigned performance of these steps to third parties, such as its customers, agents or contractors, the third parties act vicariously as agents of the Counter-Defendants, or form a joint enterprise with Counter-Defendants, to infringe at least Claim 1 of the '088 Patent. Alternatively, the Counter-Defendants contract with the third parties to perform the infringing steps. Counter-Defendants profit vicariously from third party infringement, condition the third parties' participation and receipt of benefits of the Vault application on the performance on the infringing activity and further establish the respective timing and manner of the third parties' performance of the infringing activity.

97. Counter-Defendants also form a joint enterprise among themselves, and act vicariously through each other, to infringe at least Claim 1 of the '088 Patent.

98. Counter-Defendants' infringing activities were without authority or license under the '088 Patent. Thus, Counter-Defendants have, and continue to infringe at least Claim 1 of the '088 Patent under at least 35 U.S.C. § 271(a) by their continued use, testing, manufacture, sale, offer for sale, licensing, and/or importation of the Accused Products without authority.

[28] Zoho Vault interfaces by a user using a PayPal transaction to obtain a Netflix subscription; *see* https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html; "Zoho Vault - A versatile password manager - Product Overview" https://www.youtube.com/watch?v=WcJYNh7Zjho

COUNT III: DIRECT INFRINGEMENT OF THE '901 PATENT

99. LPV realleges and incorporates by reference the allegations set forth above as if set forth verbatim herein.

100. LPV owns by assignment the entire right, title, and interest in the '901 Patent, including the right to sue for past infringement.

101. The '901 Patent was issued by the United States Patent and Trademark Office on March 23, 2021 and is titled "Methods, Apparatus and Computer Program Products for Securely Accessing Account Data". A true and correct copy of the '901 Patent is attached as Exhibit C.

102. Upon information and belief, Counter-Defendants have directly infringed and continue to directly infringe at least Claim 1 of the '901 Patent by making, using, testing (including their own use and testing), selling, offering for sale, importing and/or licensing in the United States without authority systems, products, and methods claimed by the '901 Patent, namely, the Vault application.

103. Upon information and belief, and as one illustration without limitation, Counter-Defendants infringe Claim 1 of the '901 Patent in the exemplary manners described below.

104. Counter-Defendants' Vault application provides a secure electronic "vault" including a digital wallet that allows users to store passwords and other account information as well as credit card and banking information within secure databases.

Figure 13[29]

105. The Vault application generates, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder. For example, the Vault application locally generates and stores encryption keys and account information which can then be used to conduct transactions.

29

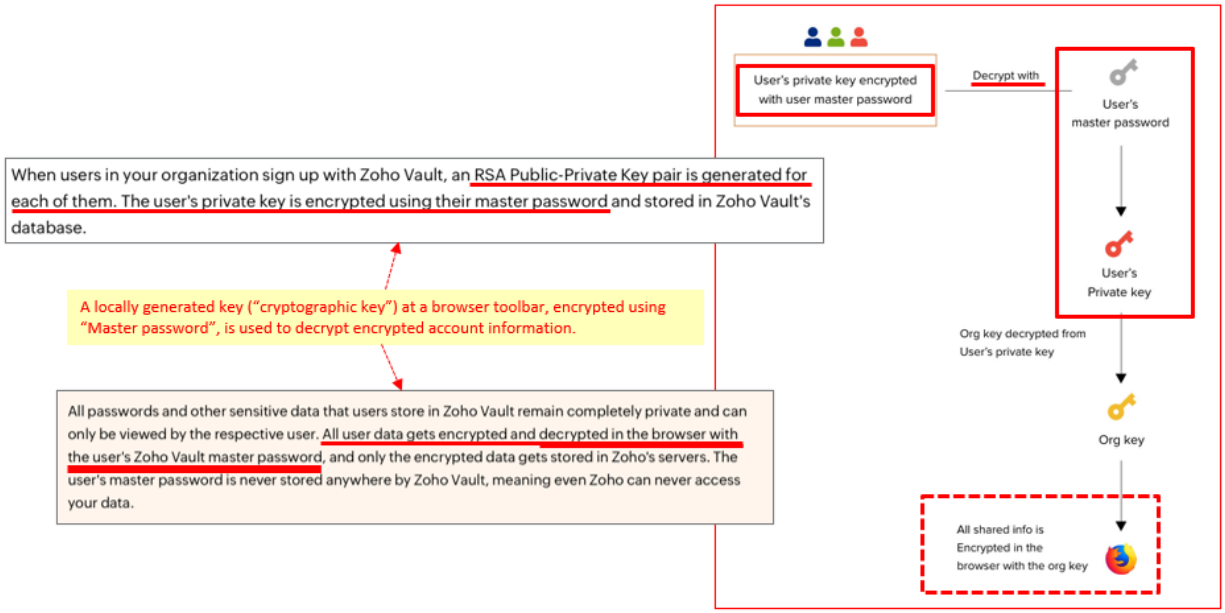
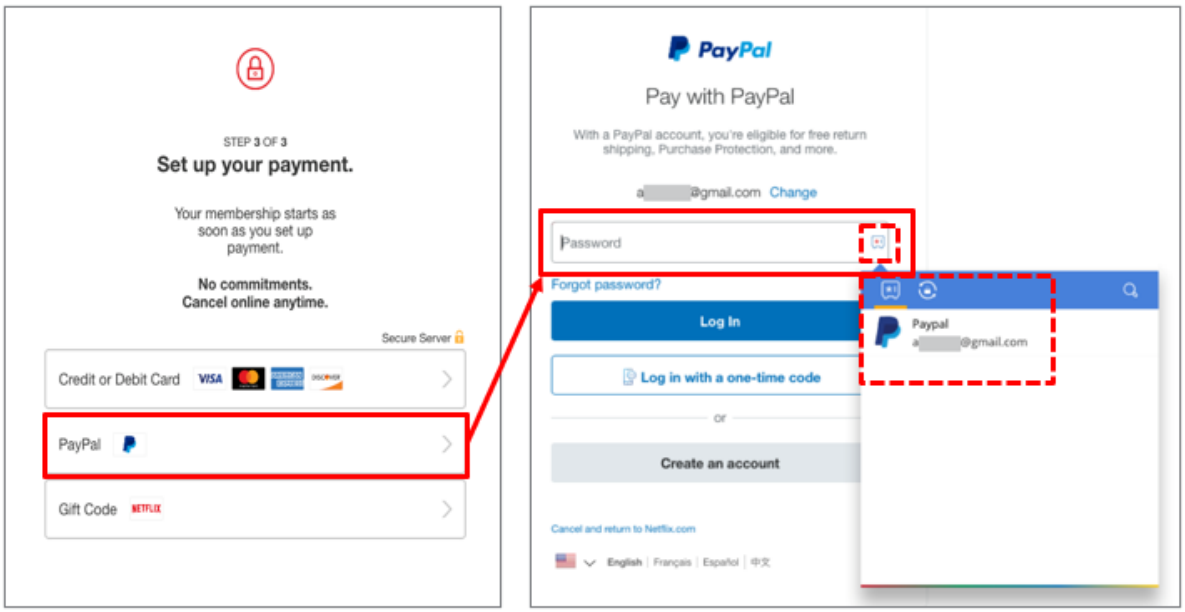


Figure 14[30]

106. The Vault application detects, by the browser toolbar, a first request to obtain the account information of the account holder. For example, the Vault application detects fields to be populated with account information ("first request") on a website and automatically populates fields with account information of user (e.g., PayPal credentials).

[30] https://www.zoho.com/vault/security.html



Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)

Figure 15[31]

107. The Vault application sends, by the browser toolbar, a second request for the account information to a secure datastore that stores the account information. For example, the Vault application sends a request ("second request") to access user account information that is stored securely in the cloud in an encrypted form. The Vault application syncs with the cloud periodically to store a local version of the encrypted data.

[31] https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html; "Zoho Vault - A versatile password manager - Product Overview" https://www.youtube.com/watch?v=WcJYNh7Zjho

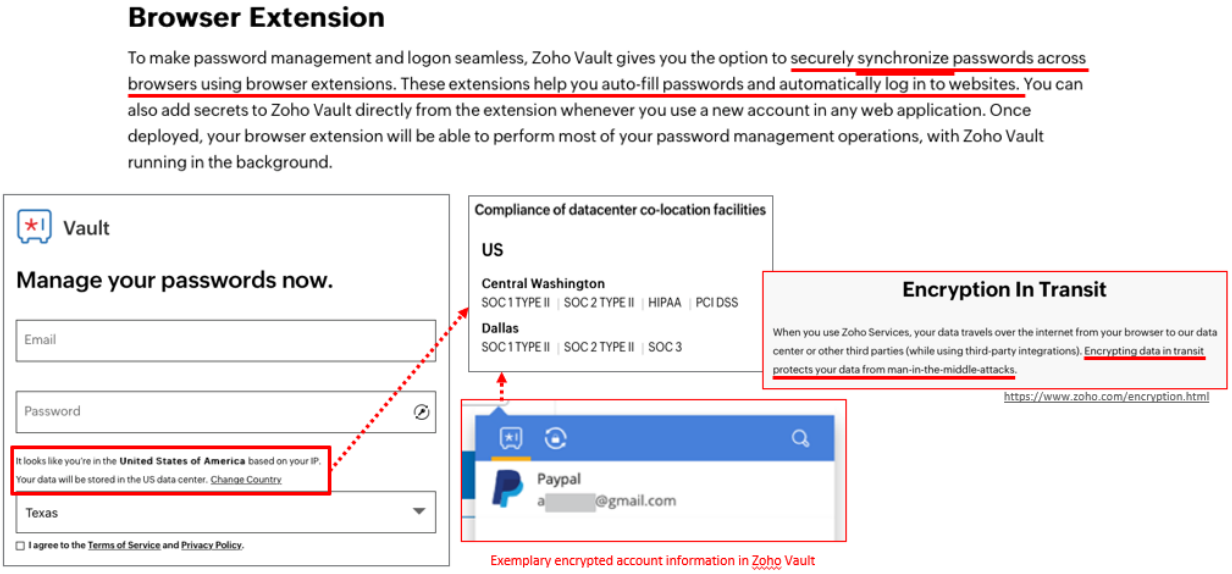


Figure 16[32]

108. The Vault application uses, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure datastore, wherein the encrypted data includes the account information. For example, the Vault application uses the locally generated user encryption key ("cryptographic key") to decrypt user account data.

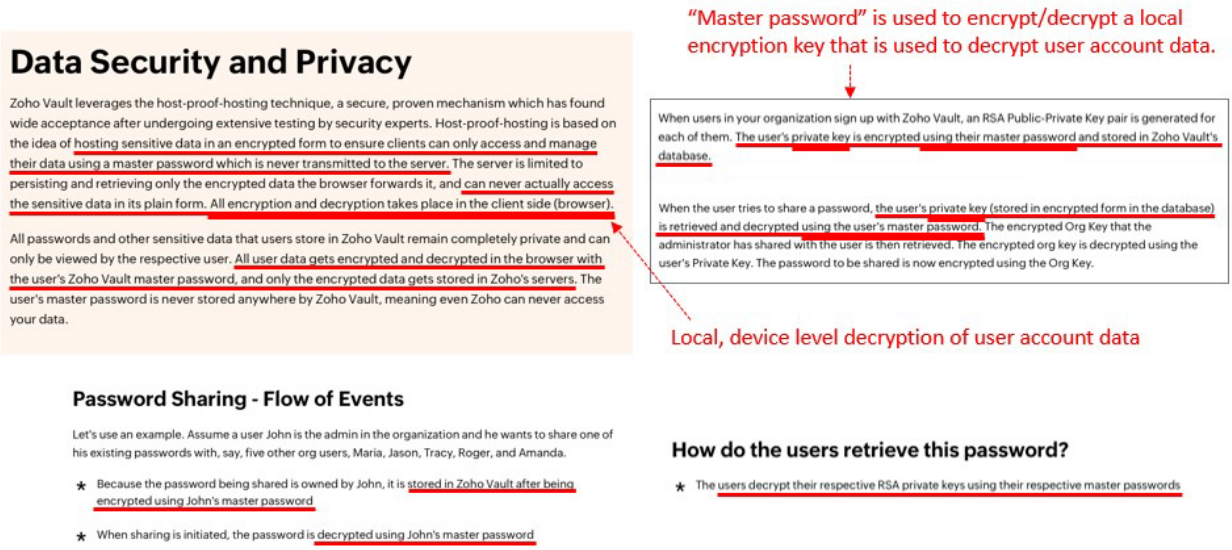


Figure 17[33]

[32] https://www.zoho.com/vault/browser-extension.html; https://www.zoho.com/know-your-datacenter.html; https://www.zoho.com/vault/signup.html; https://www.zoho.com/encryption.html
[33] https://www.zoho.com/vault/security.html

109. The Vault application securely stores, by the browser toolbar, the account information at the browser toolbar. For example, once the Vault application has decrypted user data, the raw data is stored in the temporary memory (RAM) for a limited period of time as a CPU process memory. The decrypted user data is inaccessible outside of the browser toolbar application.

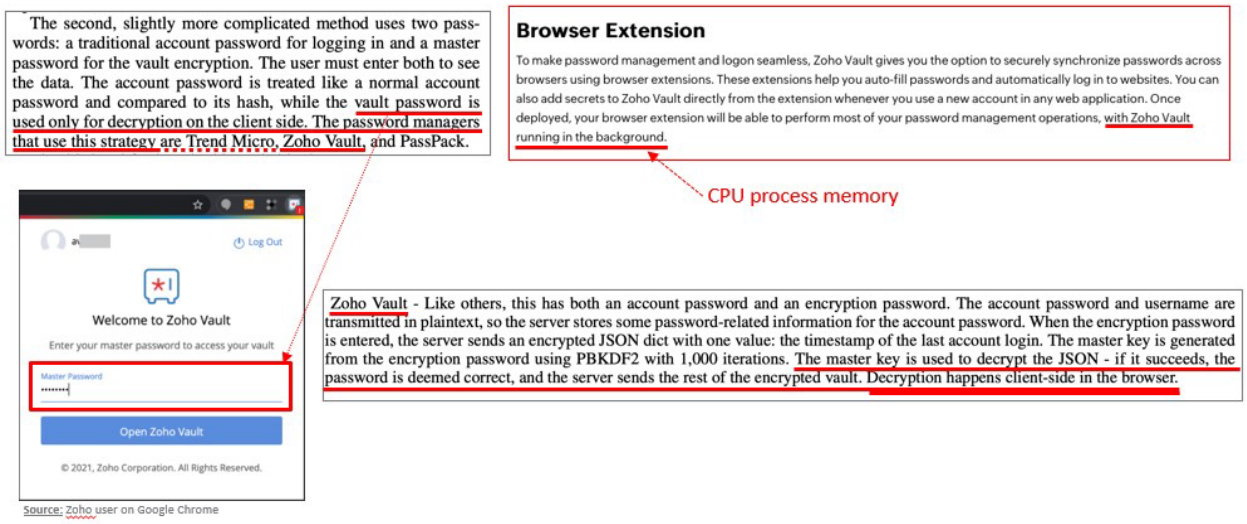


Figure 18[34]

110. The Vault application provides, by the browser toolbar, the account information to a web service in response to the first request. For example, the Vault application automatically populate fields on a website with user account information (e.g., PayPal credentials).

[34] https://www.zoho.com/vault/browser-extension.html; https://www.osti.gov/servlets/purl/1257179

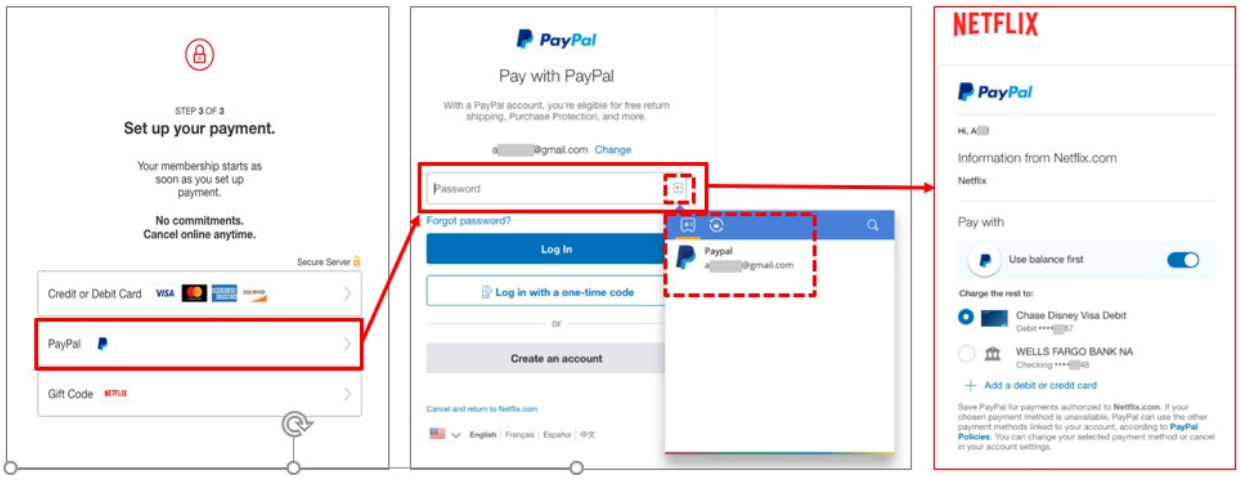


Figure 19[35]

111. To the extent that Counter-Defendants have assigned performance of these steps to third parties, such as its customers, agents or contractors, the third parties act vicariously as agents of the Counter-Defendants, or form a joint enterprise with Counter-Defendants, to infringe at least Claim 1 of the '901 Patent. Alternatively, the Counter-Defendants contract with the third parties to perform the infringing steps. Counter-Defendants profit vicariously from third party infringement, condition the third parties' participation and receipt of benefits of the Vault application on the performance on the infringing activity and further establish the respective timing and manner of the third parties' performance of the infringing activity.

112. Counter-Defendants also form a joint enterprise among themselves, and act vicariously through each other, to infringe at least Claim 1 of the '901 Patent.

113. Counter-Defendants' infringing activities were without authority or license under the '901 Patent. Thus, Counter-Defendants have, and continue to infringe at least Claim 1 of the '901 Patent under at least 35 U.S.C. § 271(a) by their continued use, testing, manufacture, sale,

[35] Zoho Vault interfaces by a user using a PayPal transaction to obtain a Netflix subscription; *see* https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html; https://help.zoho.com/portal/en/kb/vault/user-guide/articles/vault-auto-log-in-to-websites#Using_the_autofill_icon_from_the_extension

offer for sale, licensing, and/or importation of the Vault application without authority.

VI.
JURY DEMAND

114. Counterclaimant hereby demands a trial by jury of all issues so triable pursuant to Fed. R. Civ. P. 38.

VII.
PRAYER

For the reasons above, Plaintiffs respectfully requests that the Court find in its favor and against Counter-Defendants, and the Court grant Counterclaimant the following relief:

a. An adjudication that Counter-Defendants have infringed the Asserted Patents, either literally and/or under the doctrine of equivalents;

b. A judgment that LPV be awarded damages adequate to compensate it for Counter-Defendants' past infringement of the Asserted Patents, and for any continuing and future infringements, including pre-judgment and post-judgment interest costs and disbursements as justified under 35 U.S.C. § 284 and an accounting;

c. That the Court declare this to be an exceptional case and award Counterclaimant its reasonable attorneys' fees and expenses in accordance with 35 U.S.C. § 285; and

d. Any further relief that this Court deems just and proper.

Dated: March 1, 2022

Respectfully submitted,

PLATT CHEEMA RICHMOND PLLC

/s/ Matthew C. Acosta
Matthew C. Acosta
Texas Bar No. 24062577
macosta@pcrfirm.com
Andrew Lin
Texas Bar. No. 24092702
alin@pcrfirm.com
Nicholas C. Kliewer
Texas Bar No. 24083315
nkliewer@pcrfirm.com
PLATT CHEEMA RICHMOND PLLC
1201 N. Riverfront Blvd., Suite 150
Dallas, Texas 75207
214.559.2700 Main
214.559.4390 Fax

COUNSEL FOR DEFENDANT, COUNTERCLAIMANT, and THIRD-PARTY PLAINTIFF
LIBERTY PEAK VENTURES, LLC

CERTIFICATE OF SERVICE

I hereby certify that on March 1, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record, and upon all others via postage prepaid U.S. Mail.

/s/ Matthew C. Acosta
Matthew C. Acosta